Appendix E
Office of the Secretary of Defense Information Assurance Policy Robustness Levels

According to the Office of the Secretary of Defense (OSD) Global Information Grid (GIG) policy, technical Information Assurance (IA) solutions in the defense-in-depth strategy will be at one of three defined levels of robustness: high, medium, or basic, corresponding to the level of concern assigned to the system. The three levels of technical robustness solutions identified in the OSD GIG Policy are described in the following subparagraphs.

- High robustness security services and mechanisms provide the most stringent protection and rigorous security countermeasures. High robustness solutions require all of the following:
  - National Security Agency (NSA)-certified Type 1 cryptography (algorithms and implementation) for encryption, key exchange, digital signature, and hash.
  - NSA Type 1 cryptographically authenticated access control (e.g., digital signature, public key cryptography based, and challenge/response identification and authentication).
  - Key management:
    - For symmetric key, NSA-approved key management (production, control, and distribution).
    - For asymmetric key, Class 5 Public Key Infrastructure (PKI) certificates and hardware security tokens that protect the user’s private key and crypto-algorithm implementation.
  - High-assurance security design, such as specified by NSA or the International Common Criteria (CC) at a minimum an Evaluated Assurance Level (EAL) greater than 4.
  - Products evaluated and certified by NSA.

- Medium robustness security services and mechanisms provide for additional safeguards above the Department of Defense minimum. Medium robustness solutions require, at a minimum, all of the following:
  - National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) validated cryptography (algorithms and implementation) for encryption, key exchange, digital signature, and hash (see algorithms at Table 5-4).
  - NIST cryptographically authenticated access control (e.g., digital signature, public key cryptography based, and challenge/response identification and authentication).
  - Key management:

    - ➢ For symmetric key, NSA-approved key management (production, control, and distribution).
  - – For asymmetric key, Class 4 PKI certificates and hardware security tokens that protect the user's private key.
  - – Good assurance security design, such as specified in CC as EAL3 or greater.
  - – Solutions evaluated and validated under the Common Criteria Evaluation validation scheme or NSA.

- Basic robustness solutions are equivalent to good commercial practice. Basic robustness require, at a minimum, all of the following:
  - – NIST FIPS validated cryptography (algorithms and implementation) for encryption, key exchange, digital signature, and hash (see algorithms at Table 5-4).
  - – Authenticated access control (e.g., digital signature, public key cryptography based, challenge/response identification and authentication, or preplaced keying material).
  - – Key management:
    - ➢ For symmetric key, NIST-approved key management (production, control and distribution).
    - ➢ For asymmetric key, Class 3 PKI certificates or preplace keying material. See reference (p) for policy on migration to Class 4 certificates and software tokens (private keys held in software on the user's workstation).
  - – CC EAL 1 or greater assurance.
  - – Solutions evaluated and validated under the National Information Assurance Partnership (NIAP) CC Evaluation Validation Scheme or NSA.

The OSD GIG Policy indicates that the robustness of a network solution must be considered in the context of defense-in-depth and the threat environment in which the system operates. For instance, a system operating on a protected backbone between secure enclaves may not require additional mechanisms for authentication and access control. In addition, if community of interest separation is provided through encryption, it will require less robust solutions.